UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/889,410	07/17/2001	J Kitahara	H-996	2813

7590 11/07/2005

EXAMINER	
SCHUBERT, KEVIN R	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 11/07/2005

John R Mattingly
Mattingly Stanger & Malur
1800 Diagonal Rd
Suite 370
Alexandria, VA 22314

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/889,410	KITAHARA, J	
	Examiner	Art Unit	
	Kevin Schubert	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10/21/05*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9 and 14-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9 and 14-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-9 and 14-19 have been considered.

Allowable Subject Matter

Claim 18 would be allowable if rewritten to overcome the rejection(s) under 35 U.S.C. 112, 2nd paragraph, set forth in this Office action and to include all of the limitations of the base claim and any intervening claims.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claim 19 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The examiner finds no support for the limitations of claim 19 in the Specification. The examiner requires that the applicant make appropriate correction or provide the examiner with a specific passage which discloses the limitations of the claim.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 9 and 16 are rejected under 35 USC 112, second paragraph. Claim 9 recites the limitation "said generated key information" in part d. There is insufficient antecedent basis for this limitation in the claim. In independent claim 1, applicant discloses the generation of first key information

and second key information. It is not clear what the applicant is referencing with "said generated key information". Claim 16 is rejected accordingly for being dependent on claim 9. Appropriate correction is required.

Claim 18 is rejected under 35 USC 112, second paragraph, as being dependent on rejected claim 17.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-2,4-5,7,9,14, and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Heer, U.S. Patent No. 5,999,629, in view of Imai, U.S. Patent No. 5,512,977, in further view of Stokes, U.S. Patent No. 6,473,861.

As per claim 1, the applicant describes an information processing apparatus including the following limitations which are met by Heer in view of Imai in further view of Stokes:

a) a processing device for performing predetermined processing of information (Heer: Col 3, line 62 to Col 4, line 15, Fig 1);

b) a bus for interconnecting said processing device and other component devices of said information processing apparatus (Heer: Col 3, line 62 to Col 4, line 15, Fig 1);

c) wherein said processing device is integrated on a single semiconductor chip, internally generates first key information and second key information, internally encrypts sensitive information inputted from said bus with said generated second key information, internally encrypts said generated

second key information with said generated first key information, and outputs said encrypted sensitive information and said encrypted second key information to said bus without outputting said first key information used for encrypting said second key information to said bus (Heer: Col 3, line 62 to Col 4, line 15; Fig 1);

d) wherein said processing device newly generates different second key information each time sensitive information inputted from said bus is encrypted (Imai: Col 2, line 15-18);

e) wherein said first key information is common to a plurality of said second key information (Heer: Col 3, line 62 to Col 4, line 15; Fig 1);

f) wherein said processing device deletes said first key information in said single semiconductor chip if an abnormality is detected (Stokes: Col 6, line 56-67);

Heer discloses all the limitations of the above claim except for limitations d) and f). Imai discloses limitation d) in a system which newly generates key information for each encryption process. Combining Imai with Heer allows for the generation of new key information each time sensitive information is input. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Imai with those of Heer and newly generate key information for each encryption process because the hacker has less of an opportunity to steal the encryption key because it is newly generated with each encryption process.

Heer in view of Imai does not disclose that the processing device deletes key information if an abnormality is detected. Stokes discloses this limitation in a system in which key information is erased if an abnormality is detected. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Stokes with those of Heer in view of Imai because doing so prevents key information from being obtained by an unauthorized entry into the system.

As per claim 2, the applicant describes the information processing apparatus of claim 1, which is met by Heer in view of Imai in further view of Stokes, with the following limitation which is met by Heer:

Wherein said processing device comprises an external bus controller for preventing non-encrypted sensitive information from being output onto said bus (Heer: Col 3, line 62 to Col 4, line 15).

As per claim 4, the applicant describes the information processing apparatus of claim 1, which is met by Heer in view of Imai in further view of Stokes, with the following limitation which is met by Heer:

Wherein a memory device is provided for storing information encrypted by said processing device (Heer: Col 3, line 62 to Col 4, line 15).

As per claim 5, the applicant describes the information processing apparatus of claim 1, which is met by Heer in view of Imai in further view of Stokes, with the following limitation which is met by Heer:

Wherein said processing device comprises means for decrypting encrypted information at an information write operation (Heer: Col 3, line 62 to Col 4, line 15).

As per claim 7, the applicant describes the information processing apparatus of claim 1, which is met by Heer in view of Imai in further view of Stokes, with the following limitation which is met by Heer:

Wherein a plurality of said processing devices are provided, and cryptographic processing is carried out in each of said processing devices (Heer: Fig 1).

As per claim 9, the applicant describes the information processing apparatus of claim 1, which is met by Heer in view of Imai in further view of Stokes, with the following limitations which are met by Heer and Stokes:

a) a microprocessor for carrying out said predetermined processing (Heer: Col 3, lines 4-9);

b) a generator for generating said key information (Heer: Col 3, lines 4-9);

c) a cryptographic algorithm memory device for storing an algorithm for information cryptographic processing (Heer: Col 3, lines 4-9);

d) a volatile memory device for storing said generated key information (Stokes: Col 7, lines 51-52);

e) a cryptographic processing device for carrying out cryptographic processing with said stored key information according to said algorithm (Heer: Col 3, line 62 to Col 4, line 15);

f) a microprocessor bus for interconnecting said microprocessor, said generator, said cryptographic processing algorithm memory device, said volatile memory device and said cryptographic processing device (Heer: Col 3, lines 4-9; Fig 1);

g) wherein a power supply to said volatile memory is stopped so as to delete said key information in said single semiconductor chip if said abnormality is detected (Stokes: Col 7, lines 51-52).

As per claim 14, the applicant describes the information processing apparatus as claimed in claim 1, which is met by Heer in view of Imai in further view of Stokes, with the following limitation which is met by Stokes:

Wherein said abnormality is a disassembly or removal of a case or housing of said processing device (Stokes: Col 4, lines 12-24).

As per claim 19, the applicant describes the information processing apparatus of claim 1, which is met by Heer in view of Imai in further view of Stokes, with the following limitation which is met by Heer:

a) wherein said processing device receives an encrypted application program from said bus upon starting of said information processing apparatus, decrypts said encrypted application program, generates said sensitive information by executing said decrypted application program, internally encrypts said generated sensitive information with said generated second key information, and outputs said encrypted sensitive information and said encrypted second key information to said bus without outputting said first key information to said bus (Heer: Col 3, line 62 to Col 4, line 15).

Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Heer in view of Imai in further view of Stokes in further view of Hartman, U.S. Patent No. 5,224,166.

As per claim 3, the applicant describes the information processing apparatus of claim 2, which is met by Heer in view of Imai in further view of Stokes, with the following limitation which is met by Hartman:

Wherein information not requiring encryption is output onto said bus through said external bus controller (Hartman: Col 5, lines 35-44);

Heer in view of Imai in further view of Stokes disclose all the limitations of claim 2. However, Heer in view of Imai in further view of Stokes do not disclose that information not requiring encryption is output onto said bus through an external bus controller. Hartman discloses this limitation. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Hartman with those of Heer in view of Imai in further view of Stokes because it is sometimes necessary for information not requiring encryption to be output to the bus.

Claims 6 and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Heer in view of Imai in further view of Stokes in further view of Davis, U.S. Patent No. 5,805,712.

As per claims 6 and 8, the applicant describes the information processing apparatus of claims 5 and 1, which is met by Heer in view of Imai in further view of Stokes, with the following limitations which are met by Davis:

a) wherein said information processing apparatus is connected to a different information processing apparatus through a network (Davis: Col 10, lines 11-15);

b) wherein said information processing apparatus decrypts encrypted information which is received from said different information processing apparatus (Davis: Col 3, lines 27-30);

Heer in view of Imai in further view of Stokes discloses all the limitations of claim 5. However Heer in view of Imai in further view of Stokes does not disclose the limitations above. Davis discloses these limitations in a system in which encrypted data is received over a network. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Davis with those of Heer in view of Imai in further view of Stokes because doing so allows for the reception of data over a network.

Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Heer in view of Imai in further view of Stokes in further view of Nagai, U.S. Patent No. 6,571,263.

As per claim 15, the applicant describes the information processing apparatus of claim 1, which is met by Heer in view of Imai in further view of Stokes, with the following limitations which are met by Heer and Nagai:

a) wherein said key information is a random number (Heer: Col 3, lines 6-7);

b) wherein said generator generates said random number based on a signal outputted from a constant voltage diode (Nagai: 8 of Fig 1);

Heer in view of Imai in further view of Stokes disclose all the limitations of claim 1. However, Heer in view of Imai in further view of Stokes do not disclose the use of a constant voltage diode in random number generation.

Nagai discloses a random number generator apparatus which includes the use of a zener diode, which is a constant voltage diode. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Nagai with those of Heer in view of Imai in further view of Stokes and add the use of a constant voltage diode because constant voltage diodes are commonly used and known to provide a good means for random number generation.

Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Heer in view of Imai in further view of Stokes in further view of Koizumi, U.S. Patent No. 5,892,974, in further view of Yamamoto, U.S. Patent No. 5,990,873.

As per claim 17, the applicant describes the information processing apparatus of claim 1, which is met by Heer in view of Imai in further view of Stokes, with the following limitation which is met by Koizumi and Yamamoto:

Wherein said processing device comprises a battery backed first RAM for storing said generated first key information and a second RAM for storing said generated second key information, said second RAM including a working area (Koizumi: Col 8, liens 35-54; Yamamoto: Col 3, lines 50-57);

Heer in view of Imai in further view of Stokes disclose all the limitations of claim 1. Heer in view of Imai in further view of Stokes do not disclose a first and second RAM. Koizumi discloses the use of a first and second RAM. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Koizumi with those of Heer in view of Imai in further view of Stokes because having a first and second RAM makes the system more robust by having more opportunity for storage and maintenance of stored data.

Heer in view of Imai in further view of Stokes in further view of Koizumi do not disclose that the RAM is battery-backed. Yamamoto discloses this feature. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Yamamoto with those of Heer in view of Imai in further view of Stokes in further view of Koizumi because having RAM be battery-backed allows for the information processing apparatus to be dependent on a battery rather than a separate source of power, which may be useful, for example, in a portable system.

Response to Arguments

Applicant's arguments with respect to claim 1 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH

shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally be reached on M-F 7:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KS

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER